Отчёт по лабораторной работе №7

Управление журналами событий в системе

Анна Саенко

Содержание

# 1 Цель работы

Получить навыки работы с журналами мониторинга различных событий в системе.

# 2 Ход выполнения работы

## 2.1 Мониторинг журнала системных событий в реальном времени

Сначала я открыла три вкладки терминала и в каждой получила полномочия администратора, выполнив команду su -.

Во второй вкладке я запустила мониторинг системных сообщений в реальном времени при помощи команды tail -f /var/log/messages.  
На скриншоте показаны примеры сообщений, которые были зафиксированы в логе.

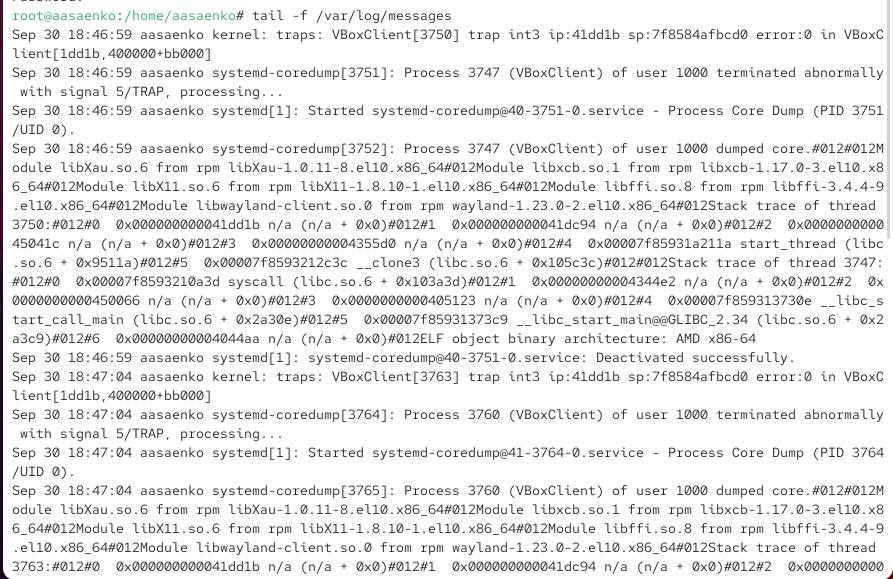


Рис. 1: Мониторинг системных сообщений в реальном времени

Затем в третьей вкладке я вернулась к своей учётной записи, нажав Ctrl + d, и попыталась получить права суперпользователя, но специально ввела неправильный пароль.  
В результате во второй вкладке появилось сообщение о неудачной попытке входа.

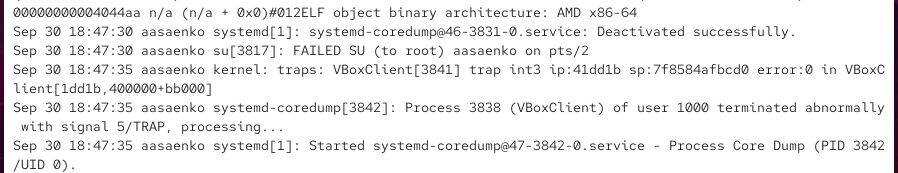


Рис. 2: Ошибка при вводе неверного пароля

После этого я ввела команду logger hello.  
Сообщение «hello» сразу отобразилось в окне мониторинга системных сообщений.

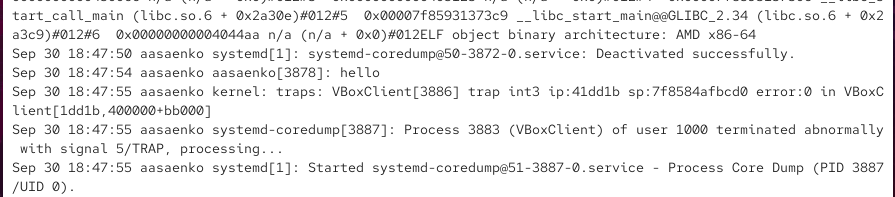


Рис. 3: Регистрируемое сообщение hello

Затем я остановила мониторинг файла /var/log/messages сочетанием клавиш Ctrl + C и просмотрела последние 20 строк журнала безопасности командой tail -n 20 /var/log/secure.  
В журнале сохранились записи о неудачных попытках авторизации при использовании команды su.

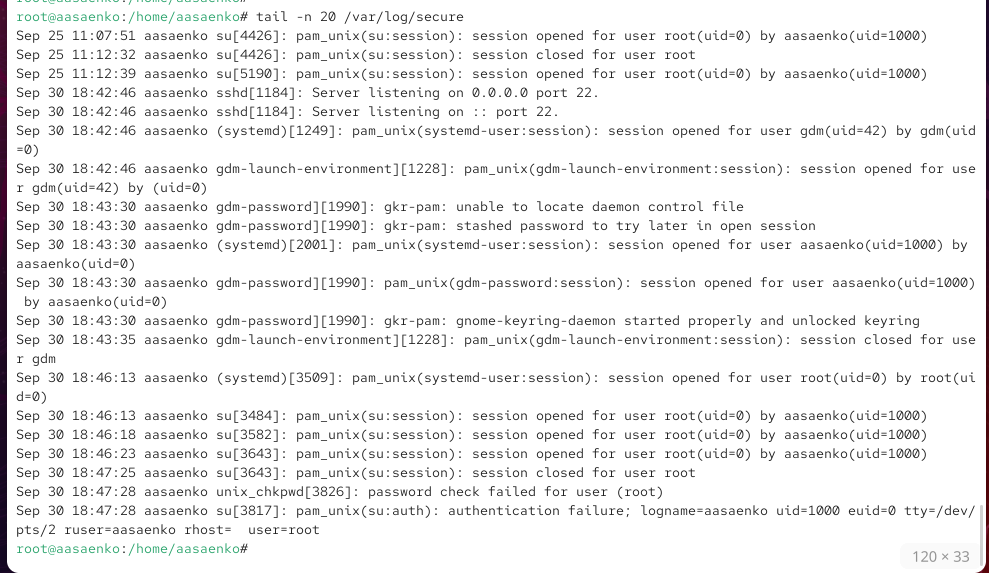


Рис. 4: Просмотр файла secure

## 2.2 Изменение правил rsyslog.conf

Сначала я установила веб-сервер Apache при помощи пакетного менеджера dnf.  
После завершения установки я запустила веб-службу и добавила её в автозагрузку.

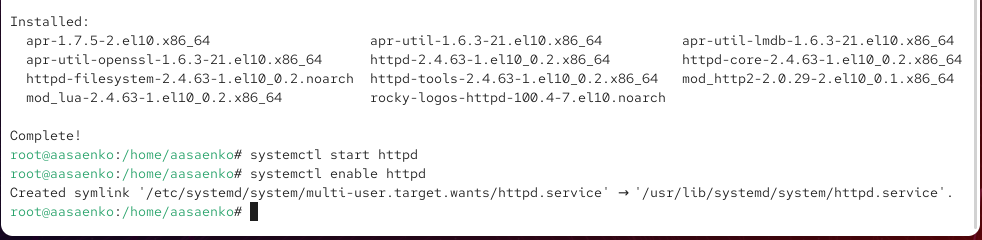


Рис. 5: Установка и запуск httpd

Во второй вкладке терминала я открыла журнал ошибок веб-сервера командой tail -f /var/log/httpd/error\_log.  
На скриншоте видно, что служба httpd успешно запущена и функционирует.

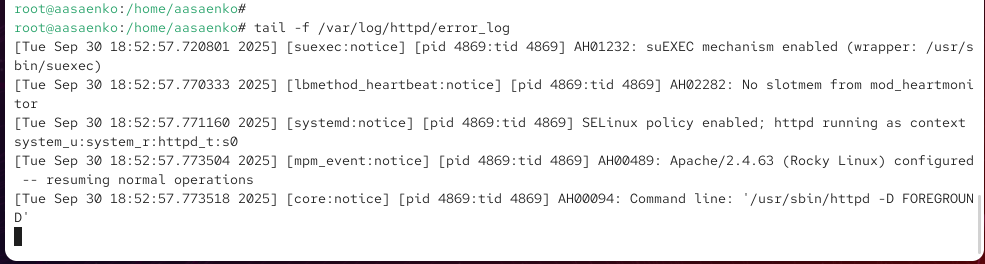


Рис. 6: Мониторинг журнала ошибок Apache

Затем я отредактировала файл конфигурации /etc/httpd/conf/httpd.conf.  
В конец файла я добавила строку ErrorLog syslog:local1, чтобы сообщения об ошибках веб-службы перенаправлялись в системный журнал через объект **local1**.

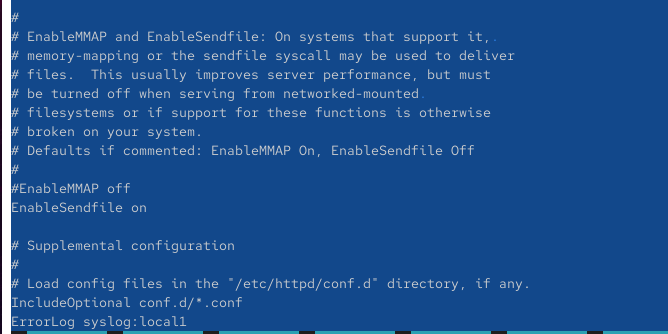


Рис. 7: Добавление параметра ErrorLog в конфигурацию Apache

После этого в каталоге /etc/rsyslog.d я создала новый файл httpd.conf.  
Эта настройка позволила перенаправлять все сообщения от объекта **local1** в отдельный лог-файл /var/log/httpd-error.log.

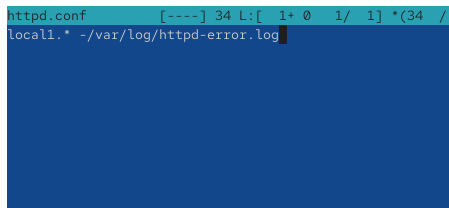


Рис. 8: Создание правила для перенаправления логов Apache

Затем я перезапустила службы rsyslog и httpd, чтобы изменения вступили в силу.  
После этого я создала дополнительный файл debug.conf с правилом записи отладочных сообщений в файл /var/log/messages-debug.

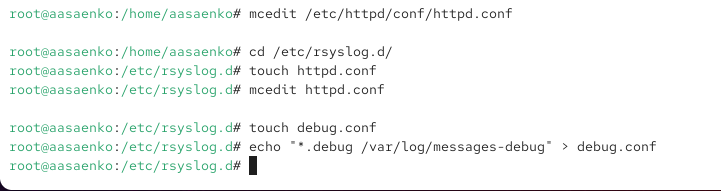


Рис. 9: Создание правил для отладочного логирования

Во второй вкладке терминала я запустила мониторинг отладочных сообщений с помощью tail -f /var/log/messages-debug.  
Затем в третьей вкладке я сгенерировала сообщение отладки с помощью команды logger -p daemon.debug "Daemon Debug Message".  
Сообщение успешно отобразилось в файле /var/log/messages-debug.

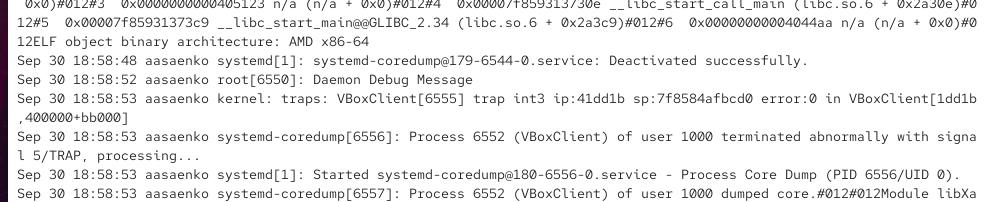


Рис. 10: Мониторинг и регистрация отладочного сообщения

## 2.3 Использование journalctl

Сначала я просмотрела содержимое системного журнала с момента последнего запуска системы, используя команду journalctl.  
Для пролистывания журнала я применяла клавиши Enter и Space, а для выхода — q.

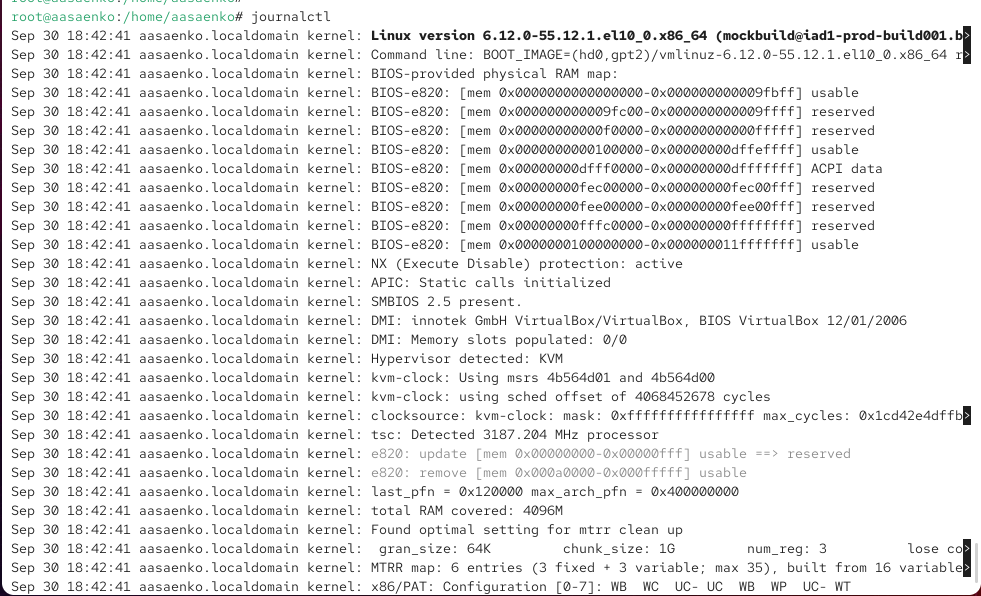


Рис. 11: Просмотр журнала событий

Далее я вывела журнал без использования пейджера при помощи ключа --no-pager.

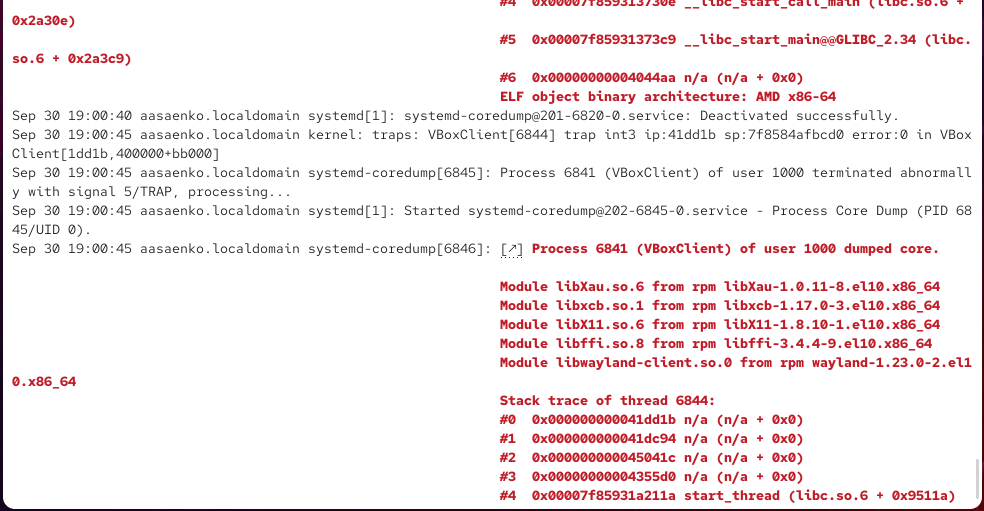


Рис. 12: Вывод журнала без пейджера

Затем я перешла в режим просмотра журнала в реальном времени, выполнив команду journalctl -f.  
Для завершения мониторинга я использовала сочетание клавиш Ctrl + C.

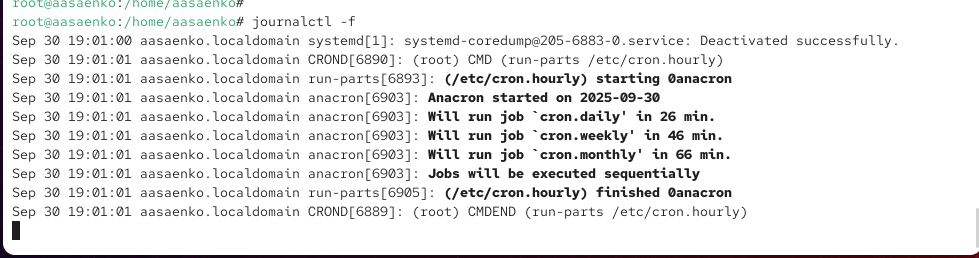


Рис. 13: Режим реального времени в journalctl

Чтобы ознакомиться с параметрами фильтрации, я ввела команду journalctl и дважды нажала клавишу Tab.  
В терминале появился список доступных опций.

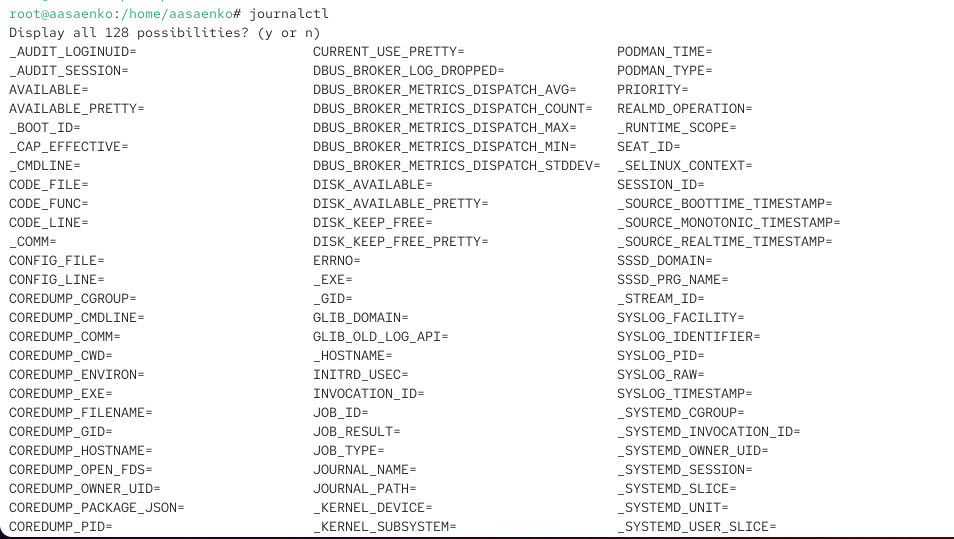


Рис. 14: Просмотр доступных параметров фильтрации

После этого я просмотрела события, относящиеся к пользователю с UID 0, выполнив команду journalctl \_UID=0.

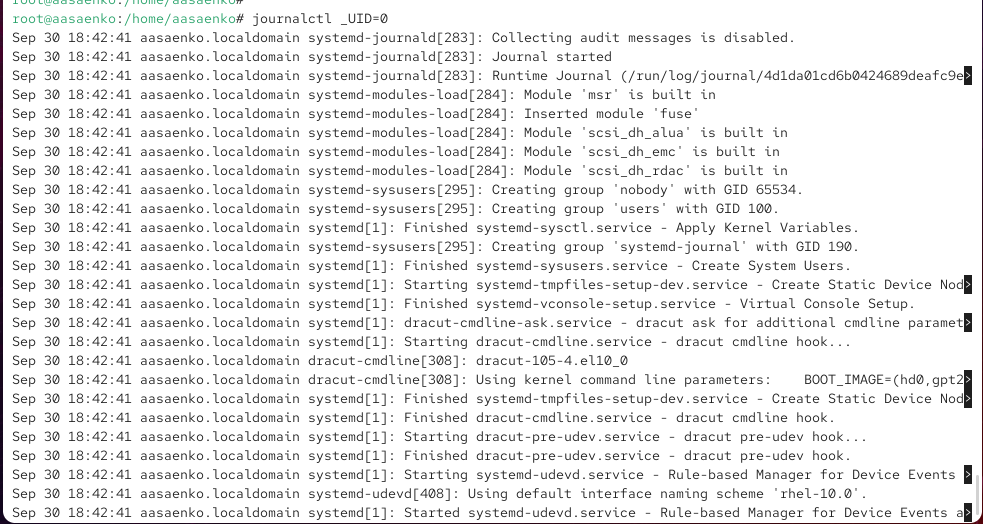


Рис. 15: Фильтрация журнала по UID

Для отображения последних 20 строк журнала я использовала команду journalctl -n 20.

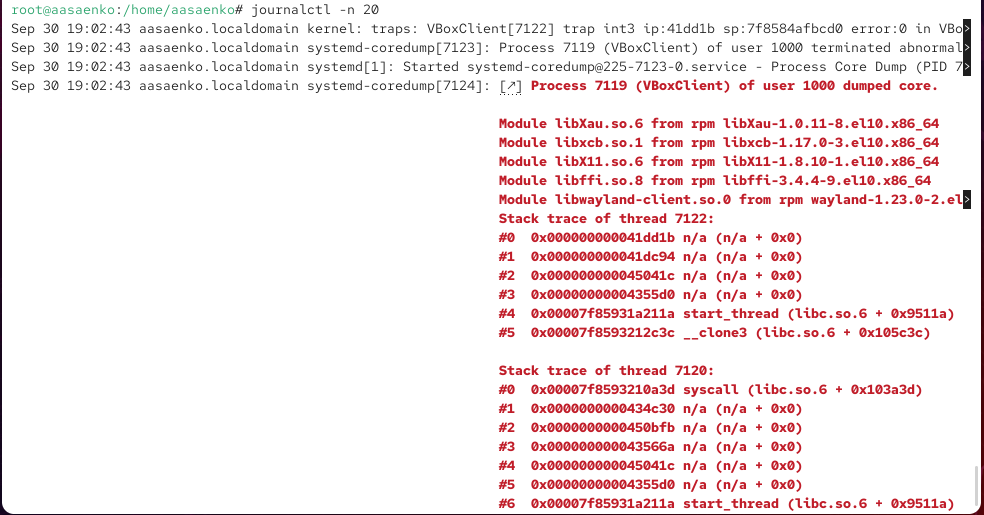


Рис. 16: Просмотр последних 20 строк журнала

Затем я вывела только сообщения об ошибках при помощи команды journalctl -p err.

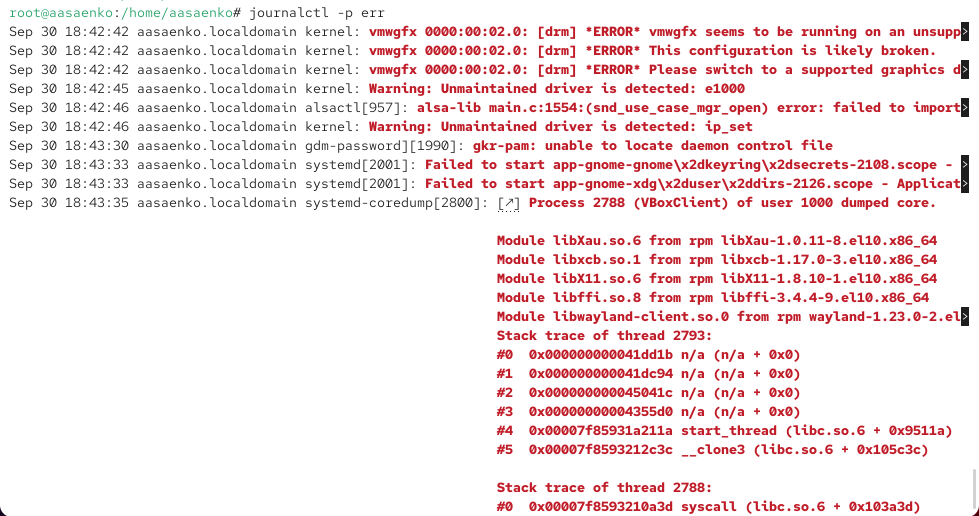


Рис. 17: Фильтрация по сообщениям с приоритетом “ошибка”

После этого я применила фильтрацию по времени и просмотрела все сообщения со вчерашнего дня с помощью команды journalctl --since yesterday.

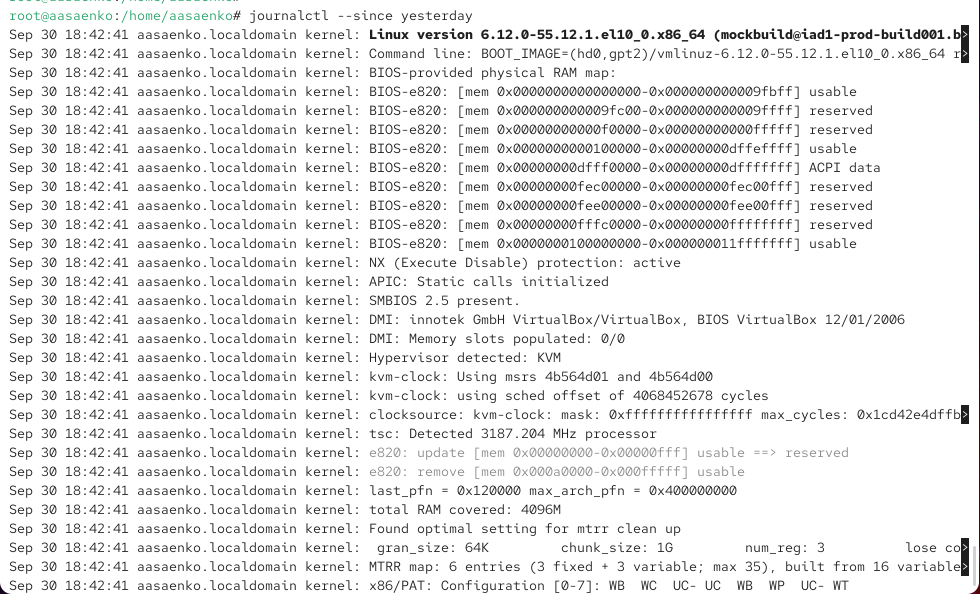


Рис. 18: Журнал со вчерашнего дня

Для просмотра только сообщений с уровнем ошибок, зафиксированных со вчерашнего дня, я выполнила команду journalctl --since yesterday -p err.

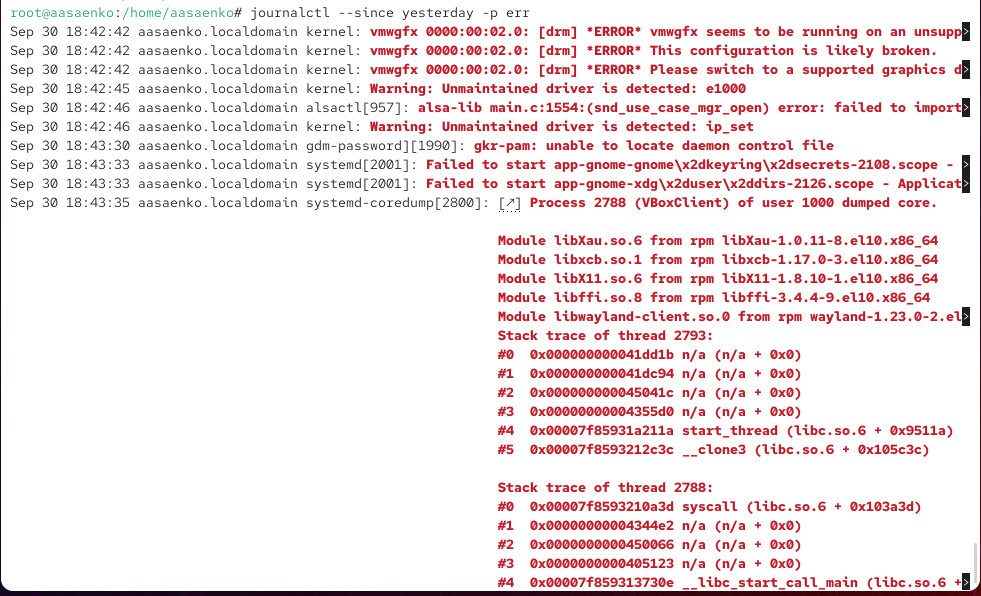


Рис. 19: Сообщения об ошибках со вчерашнего дня

Наконец, я использовала режим детализированного вывода журнала с помощью опции -o verbose.  
На скриншоте видно, что каждая запись содержит расширенную информацию о параметрах события.

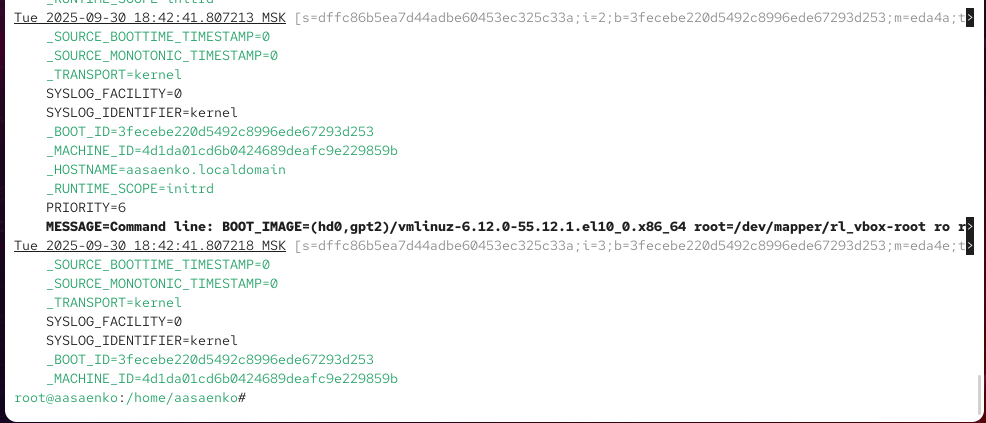


Рис. 20: Детализированный вывод журнала

Для получения сведений о работе службы sshd я применила команду  
journalctl \_SYSTEMD\_UNIT=sshd.service.  
В результате были отображены сообщения, относящиеся к запуску сервиса.

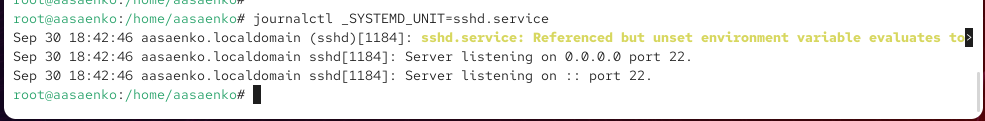


Рис. 21: Просмотр журнала для sshd

## 2.4 Постоянный журнал journald

По умолчанию система хранит логи journald во временном каталоге /run/log/journal, и они доступны только до перезагрузки.  
Чтобы сделать журнал постоянным, я выполнила следующие действия:

1. Создала каталог /var/log/journal.
2. Назначила владельца root:systemd-journal.
3. Установила права доступа 2755.
4. Применяла изменения без перезагрузки, отправив сигнал службе командой killall -USR1 systemd-journald.

После этого журнал journald стал постоянным.  
Для просмотра сообщений с момента последней перезагрузки я воспользовалась командой journalctl -b.

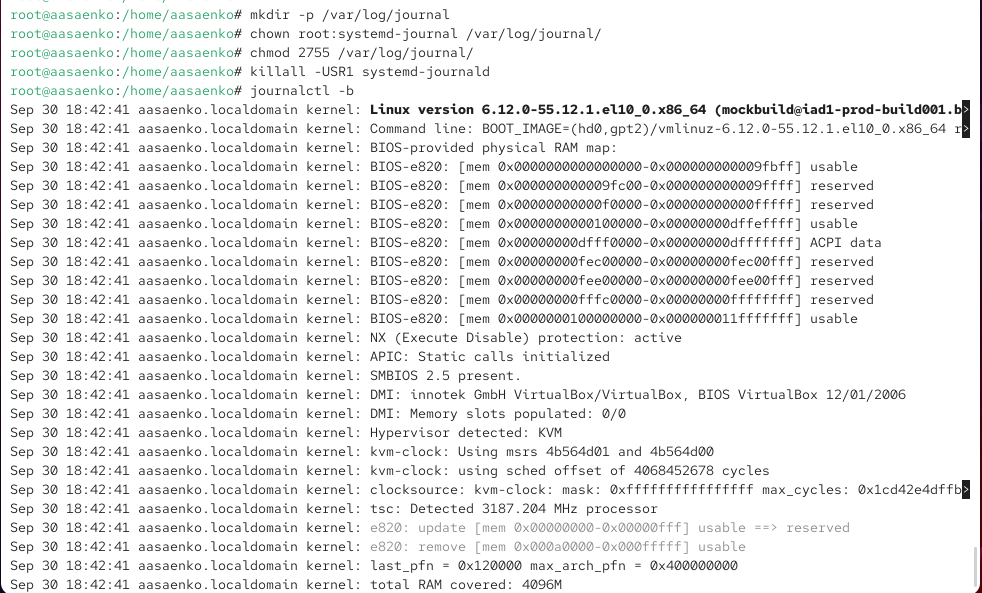


Рис. 22: Просмотр системного журнала с момента загрузки

# 3 Контрольные вопросы

1. **Какой файл используется для настройки rsyslogd?**  
   Основной конфигурационный файл находится по пути /etc/rsyslog.conf.  
   Дополнительные настройки могут храниться в каталоге /etc/rsyslog.d/.
2. **В каком файле журнала rsyslogd содержатся сообщения, связанные с аутентификацией?**  
   Сообщения, связанные с авторизацией и аутентификацией, сохраняются в файле /var/log/secure.
3. **Если вы ничего не настроите, то сколько времени потребуется для ротации файлов журналов?**  
   По умолчанию ротация файлов журналов выполняется один раз в неделю.  
   Эти параметры определяются в конфигурации logrotate, файл /etc/logrotate.conf.
4. **Какую строку следует добавить в конфигурацию для записи всех сообщений с приоритетом info в файл /var/log/messages.info?**  
   В файл конфигурации rsyslog нужно добавить строку: \*.info /var/log/messages.info
5. **Какая команда позволяет вам видеть сообщения журнала в режиме реального времени?**  
   Для мониторинга сообщений в реальном времени можно использовать:

* tail -f /var/log/messages (или другой файл журнала),
* либо journalctl -f для просмотра через systemd-journald.

1. **Какая команда позволяет вам видеть все сообщения журнала, которые были написаны для PID 1 между 9:00 и 15:00?**  
   Для этого используется фильтрация по PID и времени: journalctl \_PID=1 --since "09:00" --until "15:00"
2. **Какая команда позволяет вам видеть сообщения journald после последней перезагрузки системы?**  
   Для этого применяется команда: journalctl -b
3. **Какая процедура позволяет сделать журнал journald постоянным?**  
   Нужно создать каталог /var/log/journal, назначить ему владельца и права:

* mkdir -p /var/log/journal
* chown root:systemd-journal /var/log/journal
* chmod 2755 /var/log/journal  
  После этого отправить сигнал службе journald:
* killall -USR1 systemd-journald  
  Теперь логи будут храниться постоянно и сохраняться после перезагрузки.

# 4 Заключение

В ходе выполнения лабораторной работы я научилась использовать средства администрирования журналов в Linux.  
Были выполнены следующие действия:  
- настройка и мониторинг системных событий в реальном времени с помощью tail и logger;  
- организация перенаправления логов веб-службы Apache через rsyslog и создание отдельных файлов для отладочной информации;  
- работа с системным журналом с использованием journalctl: просмотр, фильтрация по UID, PID, времени и приоритетам сообщений;  
- настройка постоянного хранения журналов journald и проверка их сохранности после перезагрузки.

В процессе работы я закрепила знания о конфигурационных файлах /etc/rsyslog.conf, /etc/rsyslog.d/\*.conf, а также о возможностях systemd-journald. Полученный опыт показал, как можно гибко управлять логированием в системе, обеспечивать сохранность журналов и эффективно анализировать события для администрирования и диагностики.